UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,655	06/08/2001	Hovav Shacham	36321.8007.US	9498

22918 7590 05/20/2005

PERKINS COIE LLP
P.O. BOX 2168
MENLO PARK, CA 94026

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/877,655	SHACHAM ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9 and 18-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9 and 18-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/4/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 3/22/2005 was received and considered.

2. The IDS of 4/4/2005 was received and considered.

3. Claims 9, 18, 19 & 20 are pending.

Response to Arguments

4. In light of Applicant's amendments to and cancellation of the claims, the rejection of claims 1, 24-26 & 31-32 under 35 U.S.C. §112 ¶1 and the rejection of claims 1-32 under 35 U.S.C. §112 ¶2, as set forth in the previous Office Action are withdrawn.

Claim Objections

5. Claim 9 is objected to because of the following informalities:

On page 3, lines 12-13, the "determining" and "corresponding" limitations should be a single statement.

On page 3, lines 16-17, "the encryption exponents of the within the set appears to be a typographical error".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. Claims 9, 18, 19 & 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

a. The term "random" is understood to mean "randomly generated" (as is common in the art of cryptography), however, the random numbers $< r_1, r_2 >$ in the application must satisfy the conditions, $d = r_1 \bmod(p-1)$ and $d = r_2 \bmod(q-1)$, and therefore it is unclear how the numbers are random. As the claim reads, a public key is a product of two primes and two random numbers are chosen. As such, the equations each have a single definite solution, which are not necessarily equal.

b. The term $\bmod(p,q)$ is not described in the specification and therefore it is unclear what manipulations of or based on p and/or q are being performed.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 9, 18, 19 & 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

c. Regarding claims 9, 18, 19 & 20, $< r_1, r_2 >$ are not clearly related to the other elements of the claims. For the purposes of this Office Action, $< r_1, r_2 >$ are understood to be the two randomly generated numbers.

d. Regarding claims 9, 18, 19 & 20, the variables p and q are not clearly related to the other elements of the claims. For the purposes of this Office Action, p and q are understood to be the two distinct prime numbers.

e. Regarding claim 9, the limitation "wherein computational time is decreased" (p. 3, lines 5-6) is a relative limitation and therefore renders the claim indefinite.

f. Regarding claim 9, the limitation "to reduce the number of exponentiations" (p. 3, line 19) is a relative limitation and therefore renders the claim indefinite.

g. Regarding claim 9, it is unclear whether "combining", "encrypted messages", "set of encrypted messages" or "public key" comprising "an encryption exponent" (p. 3, lines 9-11).

h. Regarding claim 9, the limitation "producing a reduced number of modular inversions" (p. 4, lines 4-5) is a relative limitation and therefore renders the claim indefinite.

i. Regarding claim 9, the claim recites the limitation "the final answer" in line 15 p. 3. There is insufficient antecedent basis for this limitation in the claim.

j. Regarding claim 18, the claim recites the limitation "the first power" in line 15 of p. 4. There is insufficient antecedent basis for this limitation in the claim.

k. Regarding claim 18, the limitation "wherein a length of time of the decryption is decreased" (p. 5, lines 3-4) is a relative limitation and therefore renders the claim indefinite.

l. Regarding claim 18, the claim recites the limitation "the final answers" in line 12 of p. 5. There is insufficient antecedent basis for this limitation in the claim.

m. Regarding claim 18, the limitation "to reduce the number of exponentiations" (p. 5, line 16) is a relative limitation and therefore renders the claim indefinite.

n. Regarding claim 18, the limitation "wherein the decryption is increased by reducing the number of modular inversions" (p. 6, lines 1-2) is a relative limitation and therefore renders the claim indefinite.

o. Regarding claim 18, "wherein the decryption is increased" (p. 6, lines 1-2) is unclear.

p. Regarding claim 19, the claim recites the limitation "the first power" in line 10 of p. 6. There is insufficient antecedent basis for this limitation in the claim.

q. Regarding claim 19, the limitation "wherein a length of time of the decryption is decreased" (p. 6, line 19) is a relative limitation and therefore renders the claim indefinite.

r. Regarding claim 19, the claim recites the limitation "the k-bit values" in line 20 of p. 6. There is insufficient antecedent basis for this limitation in the claim.

s. Regarding claim 19, the claim recites the limitation "the n-bit primes" in line 21 of p. 6. There is insufficient antecedent basis for this limitation in the claim.

t. Regarding claim 20, the claim recites the limitation "the first power" in line 9 of p. 7. There is insufficient antecedent basis for this limitation in the claim.

u. Regarding claim 20, the limitation "wherein a length of time of the decryption is decreased" (p. 7, lines 18-19) is a relative limitation and therefore renders the claim indefinite.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
May 3, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100